AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means ❒ Original ❒ Duplicate Original

UNITED STATES DISTRICT COURT

for the

District of Oregon

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* Information associated with the online storage accounts stored at premises controlled by Apple, Inc., as described in Attachment A	)	Case No. 3:23-mc-477

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the Northern District of California *(identify the person or describe the property to be searched and give its location)*:

See Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B.

YOU ARE COMMANDED to execute this warrant on or before June 21, 2023 *(not to exceed 14 days)*

☑ in the daytime 6:00 a.m. to 10:00 p.m. ❒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to U.S. Magistrate Judge Youlee Yim You, via Clerk .
(United States Magistrate Judge)

❒ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

❒ for _____ days *(not to exceed 30)* ❒ until, the facts justifying, the later specific date of _____ .

Date and time issued: June 7, 2023 4:24 pm

Youlee Yim You
Judge's signature

City and state: Portland, Oregon

Hon. Youlee Yim You, United States Magistrate Judge
Printed name and title

Return

Case No.: 3:23-mc-477	Date and time warrant executed: See below dates	Copy of warrant and inventory left with: Notice Regarding Service to be filed with Court

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Date and time the acquisition of location information began:

The government acquired location information from (date and time):

to (date and time):

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A

Place to Be Searched

This warrant applies to information associated with AppleID **jaredtbates1995@gmail.com**, Directory Services Identifier **11787337509**, that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at One Apple Park Way, Cupertino, California.

ATTACHMENT B

Particular Things to Be Seized

I. Information to be disclosed by Apple

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government, in unencrypted form whenever available, for the account listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber

Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers ("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

c. All activity, connection, and transactional logs for the App Store (including purchases, downloads, and updates of Apple and third-party apps).

Apple is hereby ordered to disclose the above information to the government within 14 days of issuance of this warrant.

II. Information to Be Seized by the Government

All information described above in Section I that constitutes evidence and/or instrumentalities of violations of 18 U.S.C. § 2252A(a)(2) (Distribution of Child Pornography), from September 1, 2020, to December 31, 2020, including, for the account listed in Attachment A, information pertaining to the following matters:

a. The identity of the person(s) who created or used the Apple ID, including records that help reveal the whereabouts of such person(s);

b. Evidence indicating how and when the Apple Media Services account was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the distribution of child pornography and the account subscriber, including the application download history for the Tumblr application; and

c. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information).

III. Search Procedure

a. The warrant will be executed under the Electronic Communications Privacy Act, 18 U.S.C. § 2703(a), (b)(1)(A), and (c)(1)(A), and will require Provider to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of this attachment.

b. During its review of the information received from Provider under this warrant, law enforcement will segregate the information into two groups: (i) information that is responsive to the warrant and that the government may therefore seize; and (ii) information that is not responsive to the warrant. This review will be performed within a reasonable amount of time not to exceed 180 days from the date the warrant is executed. If the government needs additional time to conduct this review, it may seek an extension of time from the Court.

c. Information that is responsive to the warrant will be copied onto a separate storage device or medium. Responsive information may be used by law enforcement in the same manner as any other seized evidence. Information that is not responsive to the warrant will be sealed and stored on a secure medium or in a secure location. Nonresponsive information will not be reviewed again without further order of the Court (e.g., subsequent search warrant or order to unseal by the district court).

d. The government will retain a complete copy of the information received from Provider for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering with, or destroying data, and addressing

potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.